

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-244832

(43)Date of publication of application : 02.09.1994

(51)Int.Cl.

H04L 9/06

H04L 9/14

H04L 9/00

H04L 9/10

H04L 9/12

(21)Application number : 05-031514

(71)Applicant : NEC CORP

(22)Date of filing : 22.02.1993

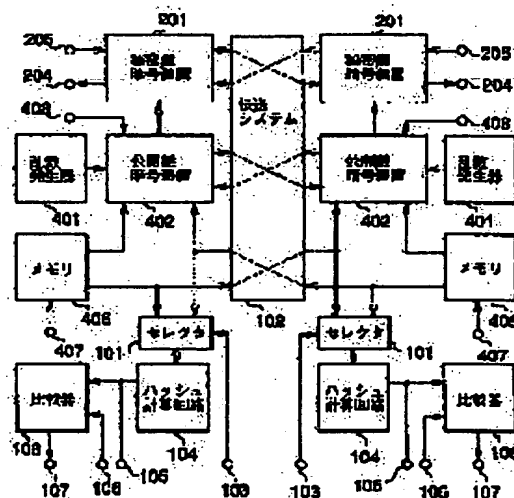
(72)Inventor : SHIMADA MICHIO

(54) SECRET INFORMATION COMMUNICATION METHOD AND SECRET INFORMATION COMMUNICATION DEVICE

(57)Abstract:

PURPOSE: To prevent the communication contents from being decoded by a third party only if numeral values which are unnecessary to be kept secret and are short in figures are set to a communication device.

CONSTITUTION: A cryptographic key to be used in a secret key cryptography device 201 is ciphered in an open key cryptography device 402 and is made to be transmitted to a communication device, and further, an open key to be used in the open key cryptography device 402 is made to be transmitted and received to/from the communication device. The hash value of the open key received by the communication device is calculated in a hash calculation circuit 104, the hash value and the hash value to be supplied from an input terminal 106 are compared in a comparator 108 and a communication is terminated if the both of them do not coincide. The hash value of the open key recorded in the communication device of a communication opposite party is preliminarily supplied to the input terminal 106.



LEGAL STATUS

[Date of request for examination] 22.02.1993

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2126012

[Date of registration] 28.01.1997

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right] 21.02.2000

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-244832

(43)公開日 平成6年(1994)9月2日

| (51)Int.Cl. ⁵ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|-----------------------------------|------|--------------------|------------------------|--------|
| H 0 4 L 9/06 9/14 9/00 | | 7117-5K 7117-5K | H 0 4 L 9/ 02 9/ 00 | Z Z |
| 審査請求 有 請求項の数 5 O L (全 9 頁) 最終頁に続く | | | | |

(21)出願番号 特願平5-31514

(22)出願日 平成5年(1993)2月22日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

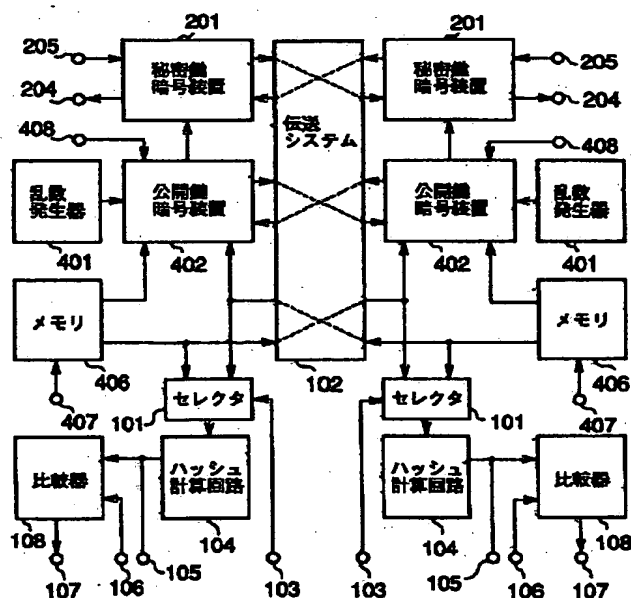
(74)代理人 弁理士 後藤 洋介 (外2名)

(54)【発明の名称】 秘密情報通信方法及び秘密情報通信装置

(57)【要約】

【目的】 秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする。

【構成】 秘密鍵暗号装置201で使用する暗号鍵を公開鍵暗号装置402で暗号化して通信装置に送信させ、さらに公開鍵暗号装置402で使用する公開鍵を通信装置に送受信させる。そして、通信装置が受信した公開鍵のハッシュ値をハッシュ計算回路104で算出して、そのハッシュ値と入力端子106から供給されるハッシュ値とを比較器108で比較し、両者が一致しなければ通信を終了する。なお、入力端子106には、予め、通信相手の通信装置に記録されている公開鍵のハッシュ値を供給しておく。



【特許請求の範囲】

【請求項1】 データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信方法において、少なくとも、公開鍵暗号の公開鍵を受信する受信ステップと、受信した公開鍵のハッシュ値を計算する計算ステップと、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較ステップと、この比較ステップにおいて両ハッシュ値が一致しない時、通信を終了する通信終了ステップとを含むことを特徴とする秘密情報通信方法。

【請求項2】 前記通信終了ステップは、両ハッシュ値が一致しない時、通信終了指示を表示する表示ステップと、通信終了指示にตอบสนองして、通信を終了するステップとを、有することを特徴とする請求項1に記載の秘密情報通信方法。

【請求項3】 前記表示ステップは、両ハッシュ値が一致しない時、前記通信終了指示を可聴表示又は可視表示することを特徴とする請求項2に記載の秘密情報通信方法。

【請求項4】 前記比較ステップは、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを表示装置に表示させて比較することを特徴とする請求項1に記載の秘密情報通信方法。

【請求項5】 データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信装置において、少なくとも、公開鍵暗号の公開鍵を受信する受信手段と、受信した公開鍵のハッシュ値を計算する計算手段と、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較手段と、この比較手段において両ハッシュ値が一致しない時、通信を終了する通信終了手段とを含むことを特徴とする秘密情報通信装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、電話やファクシミリやモデムなどの通信装置において、送信するデータを暗号化して第三者によってデータが解読されないようにするための秘密情報通信方法に関する。本発明は、更に、この秘密情報通信方法を実行する秘密情報通信装置に関する。

【0002】

【従来の技術】 通信内容が盗聴されても伝送データから送信したデータが解読されないように、データを暗号化して伝送する秘密情報通信装置としては、秘密鍵暗号にもとづく装置と公開鍵暗号にもとづく装置が広く知られ使われていた。秘密鍵暗号は対称暗号とも呼ばれ、データを暗号化するのに用いる暗号鍵と暗号化されたデータ

から元のデータを復号化するのに用いる暗号鍵が等しいものである。一方、公開鍵暗号は非対称暗号とも呼ばれ、データを暗号化するのに用いる暗号鍵と暗号化されたデータから元のデータを復号化するのに用いる暗号鍵とが異なるものである。公開鍵暗号では、復号化用の暗号鍵を決めると、それに対応する暗号化用の暗号鍵が簡単に算出できるが、暗号化用の暗号鍵からは復号化用の暗号鍵を算出できない。このため、暗号化用の暗号鍵を秘密にしなくとも、伝送データから送信内容が解読されない。この性質故に、暗号化用の暗号鍵および復号化用の暗号鍵は、それぞれ公開鍵および秘密鍵とも呼ばれる。なお、秘密鍵暗号や公開鍵暗号の一般的な原理や性質については、例えば、日経マグローウヒル社から昭和60年12月5日に出版されたデビアスとプライス (D. W. Davies and W. L. Price) 著「ネットワーク・セキュリティ」などに詳しい解説がある。

【0003】 図2は、秘密鍵暗号にもとづく秘密情報通信装置の基本構成を示すブロック図である。図において秘密鍵暗号装置201は、入力端子203から供給される暗号鍵で、入力端子205から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを伝送システム202に出力する。一方、秘密鍵暗号装置201は、入力端子203から供給される暗号鍵で、伝送システム202から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子204から出力する。伝送システム202は、秘密鍵暗号装置201から出力されるデータをもう一方の秘密鍵暗号装置201に供給する。なお、例えば公衆回線のファクシミリにおいて図2の秘密情報通信装置を用いる場合には、伝送システム202は変復調装置と公衆回線網によって構成されるが、本発明においては、伝送システム202がどのように構成されていても構わない。また、入力端子203に供給される暗号鍵は、図2の秘密情報通信装置の搭載された通信装置の使用者が、予め通信相手と打ち合わせて、通信相手が使う暗号鍵と等しいものを供給するものとする。

【0004】 図3は、図2の秘密情報通信装置において使われる、秘密鍵暗号装置201の基本構成を示すブロック図である。図において暗号化回路301は、入力端子203から供給される暗号鍵で、入力端子205から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを出力端子303から出力する。出力端子303から出力されたデータは図2の伝送システム202に供給されている。復号化回路302は、入力端子203から供給される暗号鍵で、入力端子304から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子204から出力する。入力端子304には図2の伝送システム202からデータが供給されている。

【0005】 なお、図3の暗号化装置で使われる秘密鍵

暗号としては、例えば、前記デビアスとプライスの書籍に解説されているDES (Data Encryption Standard: データ暗号化規格) 暗号や、1992年11月に水上で開催された情報理論とその応用シンポジウムの予稿集の259頁~260頁に記載された島田道雄著「多重剰余暗号」で述べられている多重剰余暗号がある。多重剰余暗号の暗号化および復号化を実行するための回路の構成方法は、特願平4-128409号明細書の暗号通信装置に記載されている。

【0006】図4は、公開鍵暗号にもとづく秘密情報通信装置の基本構成を示すブロック図である。図において秘密鍵暗号装置201は、公開鍵暗号装置402から供給される暗号鍵で、入力端子205から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを伝送システム403に出力する。一方、秘密鍵暗号装置201は、公開鍵暗号装置402から供給される暗号鍵で、伝送システム403から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子204から出力する。乱数発生器401はランダムに数値を発生し、発生した数値を公開鍵暗号装置402に供給する。メモリ406には、予め入力端子407から公開鍵暗号の秘密鍵とそれに対応する公開鍵が10 入力されて記録されており、秘密鍵が公開鍵暗号装置402に供給され、公開鍵が出力端子405から出力される。通信装置の使用者が、設定した公開鍵を忘れてしまった場合には、通信装置の使用者は、設定した公開鍵を出力端子405から読み取る。公開鍵暗号装置402の入力端子408には、公開鍵暗号装置402の搭載された通信装置が呼び出しを行った側なのかあるいは呼び出しを受けた側なのかを示す制御信号が供給されている。公開鍵暗号装置402の入力端子404には公開鍵が供給される。入力端子404に供給される公開鍵は、通信相手の通信装置のメモリ406に記録されている公開鍵と等しいもので、通信装置の使用者が予め教えあっておくものとする。そして、公開鍵暗号装置402は、公開鍵暗号装置402の搭載された通信装置が呼び出しを行った側であれば、乱数発生器401の出力した数値を秘密鍵暗号装置201に供給するとともに、メモリ406から供給される秘密鍵で、乱数発生器401の出力した数値に対して公開鍵暗号の復号化を行い、入力端子404から供給される公開鍵で、前記復号化によって得られたデータに対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを伝送システム403に出力する。一方、公開鍵暗号装置402は、通信装置が呼び出しを受けた側であれば、メモリ406から供給される秘密鍵で、伝送システム403から入力されるデータに対して公開鍵暗号の復号化を行い、入力端子404から供給される公開鍵で、前記復号化によって得られたデータに対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを秘密鍵暗号装置201に供給する。伝送

システム403は、秘密鍵暗号装置201から出力されるデータをもう一方の秘密鍵暗号装置201に供給するとともに、公開鍵暗号装置402から出力されるデータをもう一方の公開鍵暗号装置402に供給する。例えば公衆回線用のファクシミリにおいて図4の秘密情報通信装置を用いる場合には、伝送システム403は変復調装置と公衆回線網によって構成される。

【0007】なお、図4の秘密情報通信装置では、公開鍵暗号にもとづく秘密情報通信装置といっても秘密鍵暗号によってデータの暗号化を行っているが、一般に、公開鍵暗号は暗号化や復号化の速度が秘密鍵暗号に比べて遅いので、図4のようにデータは秘密鍵暗号で暗号化されて伝送され、秘密鍵暗号で使われる暗号鍵が公開鍵暗号で暗号化されて伝送される。

【0008】図5は、図4の秘密情報通信装置において使われる公開鍵暗号装置402の基本構成を示すブロック図である。図において、復号化回路502は、入力端子508から供給される秘密鍵で、入力端子509から入力されるデータに対して公開鍵暗号の復号化を行い、復号化によって得られたデータを暗号化回路503に供給する。なお、入力端子509には図4の乱数発生器401が出力する数値が、入力端子508には図4のメモリ406の出力する秘密鍵が供給されている。暗号化回路503は入力端子404から供給される公開鍵で、復号化回路502の出力に対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを出力端子506から出力する。出力端子506は図4の伝送システム403にデータを供給している。復号化回路504は、入力端子508から供給される秘密鍵で、入力端子507から入力されるデータに対して公開鍵暗号の復号化を行い、復号化によって得られたデータを暗号化回路505に供給する。入力端子506は図4の伝送システム403からデータを供給されている。暗号化回路505は、入力端子404から供給される暗号鍵で、復号化回路504から供給されるデータに対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータをセクタ501に供給する。セクタ501は、入力端子408から供給される制御信号が「通信装置が呼び出し側であること」を示していれば、入力端子509から供給されるデータを選択して出力端子505から出力し、一方、入力端子408から供給される制御信号が「通信装置が呼び出しを受けた側であること」を示していれば、暗号化回路505の出力を選択して出力端子510から出力する。出力端子510の出力は図4の秘密鍵暗号装置201に供給されている。

【0009】なお、図5の公開鍵暗号装置で使われる公開鍵暗号としては、例えば、前記デビアスとプライスの著書において解説されているRSA (Rivest Shamir and Adleman) 暗号や、例えば1991年12月に指宿で開催された第14回情報理論

とその応用シンボジウムの予稿集の第9頁から12頁に記載された島田著「もう一つの実用的な公開鍵暗号」において述べられている拡大ラビン暗号がある。また、拡大ラビン暗号の暗号化および復号化を実行するための回路の構成方法は、特願平3-268518号明細書の暗号通信符号化装置および復号化装置に記載されている。

【0010】

【発明が解決しようとする課題】しかしながら、秘密鍵暗号にもとづく暗号通信装置だと、暗号鍵が第三者に知られると通信の内容が第三者によって解読され得るので、暗号鍵を第三者に盗み見されたり盗聴されないように、信頼できる人に直接運ばせたり暗号鍵を記録したメモを封筒に厳重に封印して郵送することが必要だった。このために、暗号鍵を管理するための労力が大きいという問題があった。

【0011】公開鍵暗号にもとづく暗号通信装置では、公開鍵が第三者に知られても通信内容が解読されることはない。しかしながら、秘密鍵暗号の暗号鍵の長さが64ビットだったのに対して公開鍵暗号の公開鍵は短いものでも512ビットなので、口頭で教えたり名刺の余白に印刷することは困難であった。また、公開鍵の長さが長いために、公開鍵を通信装置に手動入力することが使用者にとって大きな負担になるという問題があった。通信装置にICカードの読み取り装置を搭載して公開鍵をICカードに記録して配布すれば公開鍵を入力する負担を減らせめものの、通信装置のコストが大きくなるという問題があった。

【0012】本発明の課題は、秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする秘密情報通信方法を提供することにある。

【0013】本発明の別の課題は、秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする秘密情報通信装置を提供することにある。

【0014】

【課題を解決するための手段】本発明によれば、データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信方法において、少なくとも、公開鍵暗号の公開鍵を受信する受信ステップと、受信した公開鍵のハッシュ値を計算する計算ステップと、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較ステップと、この比較ステップにおいて両ハッシュ値が一致しない時、通信を終了する通信終了ステップとを含むことを特徴とする秘密情報通信方法が得られる。

【0015】更に、本発明によれば、前記通信終了ステップは、両ハッシュ値が一致しない時、通信終了指示を表示する表示ステップと、通信終了指示に応答して、通信

を終了するステップとを、有することを特徴とする前述の秘密情報通信方法が得られる。

【0016】又、本発明によれば、前記表示ステップは、両ハッシュ値が一致しない時、前記通信終了指示を可聴表示又は可視表示することを特徴とする前述の秘密情報通信方法が得られる。

【0017】このように、予め通信相手から送られているハッシュ値と伝送された公開鍵のハッシュ値とが一致しなければ警報を発生して、通信を終了するか否かの判断を通信装置の使用者に行わせても良い。

【0018】更に、前記比較ステップは、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを表示装置に表示させて比較することを特徴とする前述の秘密情報通信方法が得られる。このように、予め通信相手から送られているハッシュ値と、伝送された公開鍵のハッシュ値とを表示装置に表示し、予め通信相手から送られているハッシュ値と伝送された公開鍵のハッシュ値との比較および通信を終了するか否かの判断を通信装置の使用者に行わせても良い。

【0019】又、本発明によれば、データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信装置において、少なくとも、公開鍵暗号の公開鍵を受信する受信手段と、受信した公開鍵のハッシュ値を計算する計算手段と、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較手段と、この比較手段において両ハッシュ値が一致しない時、通信を終了する通信終了手段とを含むことを特徴とする秘密情報通信装置が得られる。

【0020】

【作用】本発明では、もし盗聴者が公開鍵のハッシュ値を入手すると、原理的には、盗聴者がハッシュ値の一致するような整数を見つけ出し、その整数を公開鍵にもつような公開鍵暗号を生成できる。本発明では、公開鍵のハッシュ値のみを比較することで、受信した公開鍵が正規の通信相手から送られたものであるかどうかを確認しているので、正規の通信相手の公開鍵と盗聴者がそのようにして生成した公開鍵とを区別できない。従って盗聴者は、原理的には、正規の通信相手に成り済ましてデータを詐取できる。

【0021】この問題を解決する方法としては、ハッシュ値の生成方法を通信相手ごとに変更することが考えられる。実際、例えば前記デビアスとプライスの文献によれば、デジタル署名などの用途では、ハッシュ値の生成方法すなわちハッシュ関数の鍵が公開鍵暗号で暗号化されて、ハッシュ値と通信文とがいつしよに送信される。しかしながら、この方法では、暗号鍵の配送という問題が、ハッシュ関数の鍵の配送という問題に置き換えられるだけで意味が無い。また、ハッシュ関数の鍵を秘

密にすることも考えられるが、電話やファクシミリのように多数のメーカーによって製造され多数の装置が不特定多数に市販されている場合には、ハッシュ関数の鍵の秘密を守ることは困難である。

【0022】しかしながら、実は、ハッシュ値の生成方法を固定しておいても、正規の通信相手に成り済ましてデータを詐取することは困難である。というのも、ハッシュ値の生成方法を知っている盗聴者は、ハッシュ値が正規の通信相手と等しくなるような整数を簡単に求められるかもしれないが、公開鍵暗号においては、公開鍵から秘密鍵を求めるためには膨大な計算量を要するので、そのような整数を見つけたとしても、その整数を公開鍵とするような公開鍵暗号の秘密鍵を求めることは事実上不可能だからである。盗聴者が所望のハッシュ値を有する公開鍵と秘密鍵の組を得るには、公開鍵暗号の秘密鍵を発生して、対応する公開鍵のハッシュ値を計数するという操作を、公開鍵のハッシュ値が正規の通信相手のものと等しくなるまで繰り返すしかない。ハッシュ値の長さを64ビット程度に選んでおけば、スーパーコンピューターを使って計算しても何万年もかかるので、所望のハッシュ値を持つ公開鍵と秘密鍵の組み得ることは事実上不可能である。

【0023】

【実施例】図1は本発明にもとづく秘密情報通信方法を実行する秘密情報通信装置の基本構成を示す機能ブロック図である。図において、秘密鍵暗号装置201、公開鍵暗号装置402、乱数発生器401、メモリ406は、図4の従来の公開鍵暗号にもとづく秘密情報通信装置と同様な処理を実行する。ただし、メモリ406から出力される公開鍵は、図4の出力端子405に出力されるのではなく、伝送システム102に供給される。また、公開鍵暗号装置402は、図4の入力端子404から公開鍵を供給されるのではなく、伝送システム102から公開鍵を供給される。そして、伝送システム102は、図4の伝送システム403が行っていた処理に加えて、一方の通信装置のメモリ406が出力する公開鍵を、もう一方の通信装置の公開鍵暗号装置402に供給する。伝送システム102から供給される公開鍵とメモリ406から供給される公開鍵は、セクタ101にも供給されており、入力端子103に供給される制御信号に応じて、どちらか一方をハッシュ計算回路104に供給する。ハッシュ計算回路104は、セクタ101から供給された公開鍵のハッシュ値を生成し、ハッシュ値を出力端子105と比較器108に供給する。比較器108はハッシュ計算回路104から供給されるハッシュ値と入力端子106から供給されるハッシュ値とを比較し、もし、両者が一致していなかったら警報信号を出力端子107から出力する。なお、通信装置の使用者は、予め、入力端子103の制御信号を操作してセクタ101の出力としてメモリ406の出力を選択させ、メモ

リ406に記録された公開鍵のハッシュ値を出力端子105から得ておき、通信相手にそのハッシュ値を教える。そして、通信を行う際には、セクタ101の出力として伝送システム102の供給する公開鍵を選択させ、入力端子106に通信相手から教えられたハッシュ値を入力する。もし、伝送システム102を介して接続している通信相手のメモリ406に記録されている公開鍵のハッシュ値と、所望の通信相手のメモリ406に記録されている公開鍵のハッシュ値とが異なっていれば、比較器107は警報信号を発生する。出力端子107から出力される警報信号は、秘密情報通信装置の搭載されている通信装置によっても異なるが、多くの用途では、伝送システム102に供給され、警報信号が発生したならば伝送システム102は通信を終了する。

【0024】ただし、電話のように使用者自身がデータすなわち音声を発する通信装置では、出力端子107から出力される警報信号をブザーや発光ダイオードなどの表示装置に接続して、使用者に警報信号の有無を知らせ、通信を終了するか否かの判断を使用者に行わせることも可能である。また、電話のような通信装置では、比較器108を使わずに、ハッシュ計算回路104の出力を表示装置に表示して、ハッシュ計算回路の出力と通信相手のハッシュ値が一致するか否かの比較を使用者に行わせることも可能である。また、通信相手のハッシュ値を入力端子106から比較器108に直接供給せずに、通信相手のハッシュ値をメモリに記録しておき、メモリから比較器108に供給しても構わない。例えば、ファクシミリや電話などの通信装置では、予め使用者が通信相手の電話番号に続けて#コードで区切ってハッシュ値の十進数表示を通信装置に入力して、通信装置はその数値をメモリに登録しておき、自動ダイヤルが実行された場合には、通信装置は#コードに続いた数値を比較器108に供給することが考えられる。このようにすれば、通信を行うごとにハッシュ値を指定する必要がなくなるし、ハッシュ値が拡張された電話番号と見なせるので、秘密情報通信装置の搭載されていない電話やファクシミリを使っていたのとほぼ同様にして、秘密情報通信装置の搭載された電話やファクシミリを使える。

【0025】なお、図1のハッシュ計算回路104で使われるハッシュ値の生成方法としては、例えば前記1992年11月に水上で開催された情報理論とその応用シンポジウムの予稿集で述べられている多重剰余暗号を使うものがある。多重剰余暗号を使えば、暗号鍵のブロック長を選択するだけで、例えば長さ512ビットの公開鍵から長さ64ビットのハッシュ値を生成できる。また、多重剰余暗号の暗号化および復号化を実行するための回路の構成方法は、前記特願平4-128409号明細書の暗号通信装置に記載されている。ただし、ハッシュ計算回路104ではハッシュ値の生成方法すなわちハッシュ計算回路の鍵を固定しておくので、予め決められ

た暗号鍵を記録しておくためのメモリが必要である。

【0026】

【発明の効果】本発明の秘密通信方法及び装置では、以上で述べたように、通信装置に桁数の短いハッシュ値を指定するだけで、第三者に通信内容が解読されることなく通信できる。ハッシュ値は秘密にしておく必要が無いので、名刺などに印刷して公開したり電話を介して口頭で教えることも可能である。しかも、本発明の秘密通信方法及び装置は、従来の公開鍵暗号にもとづく秘密通信装置に公開鍵の伝送手順とハッシュ値を計算するための手段を付加するだけで済むので、実現がきわめて容易である。

【図面の簡単な説明】

【図1】本発明の秘密情報通信方法を実行する秘密情報通信装置の基本構成を示す機能ブロック図。

【図2】秘密鍵暗号にもとづく従来の秘密情報通信装置の基本構成を示す機能ブロック図。

【図3】図2の秘密情報通信装置の秘密鍵暗号装置201の基本構成を示す機能ブロック図。

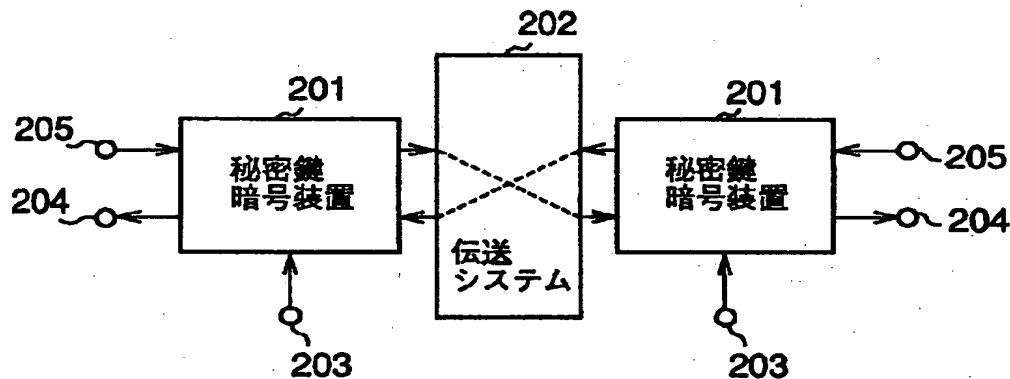
【図4】公開鍵暗号にもとづく従来の秘密情報通信装置の基本構成を示す機能ブロック図。

【図5】図4の秘密情報通信装置の公開鍵暗号装置402の基本構成を示す機能ブロック図。

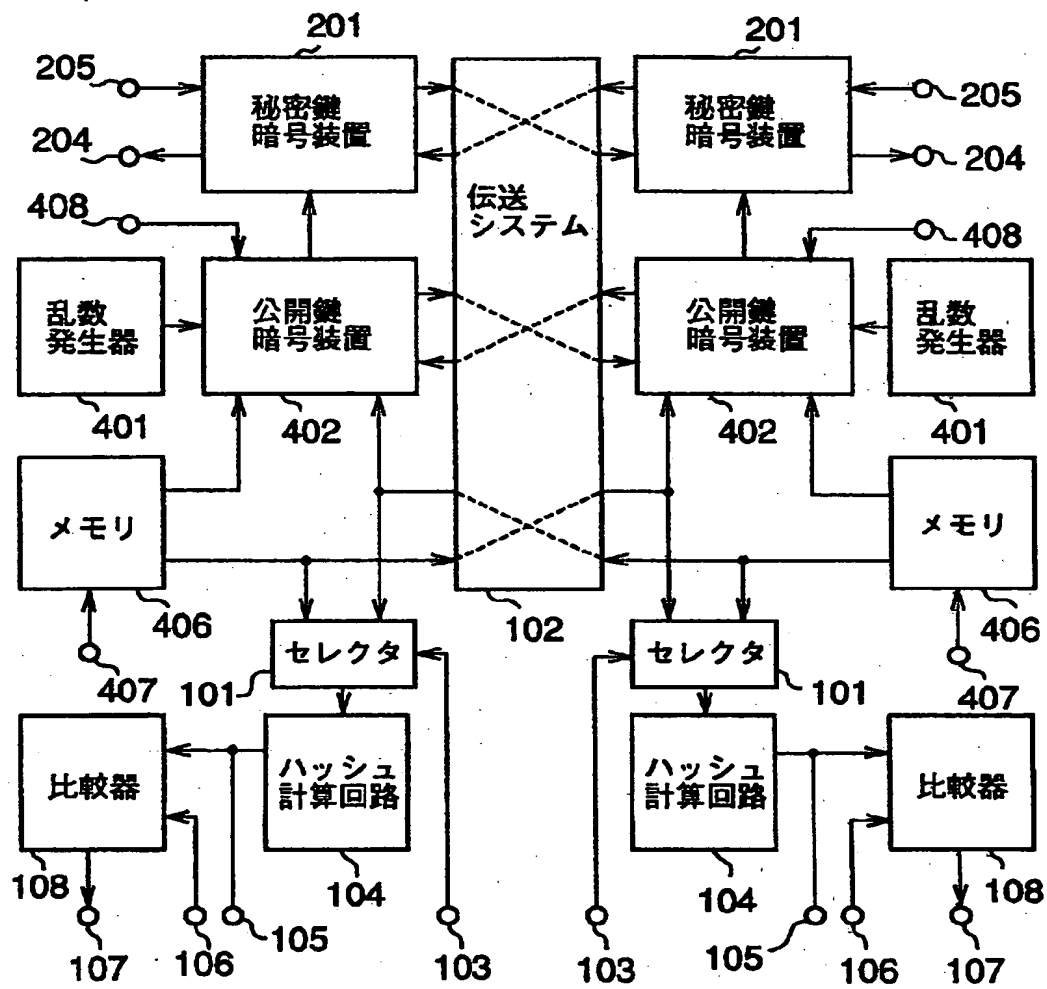
【符号の説明】

| | |
|-----|----------|
| 102 | 伝送システム |
| 104 | ハッシュ計算回路 |
| 108 | 比較器 |
| 201 | 秘密鍵暗号装置 |
| 202 | 伝送システム |
| 401 | 乱数発生器 |
| 402 | 公開鍵暗号装置 |
| 403 | 伝送システム |
| 406 | メモリ |

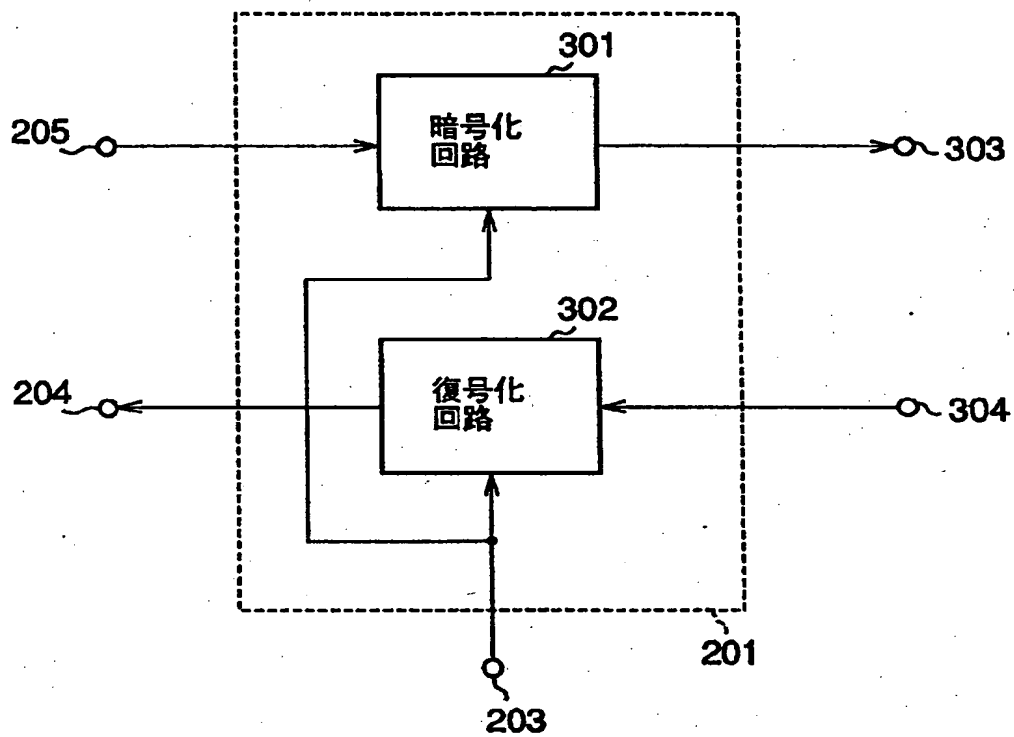
【図2】



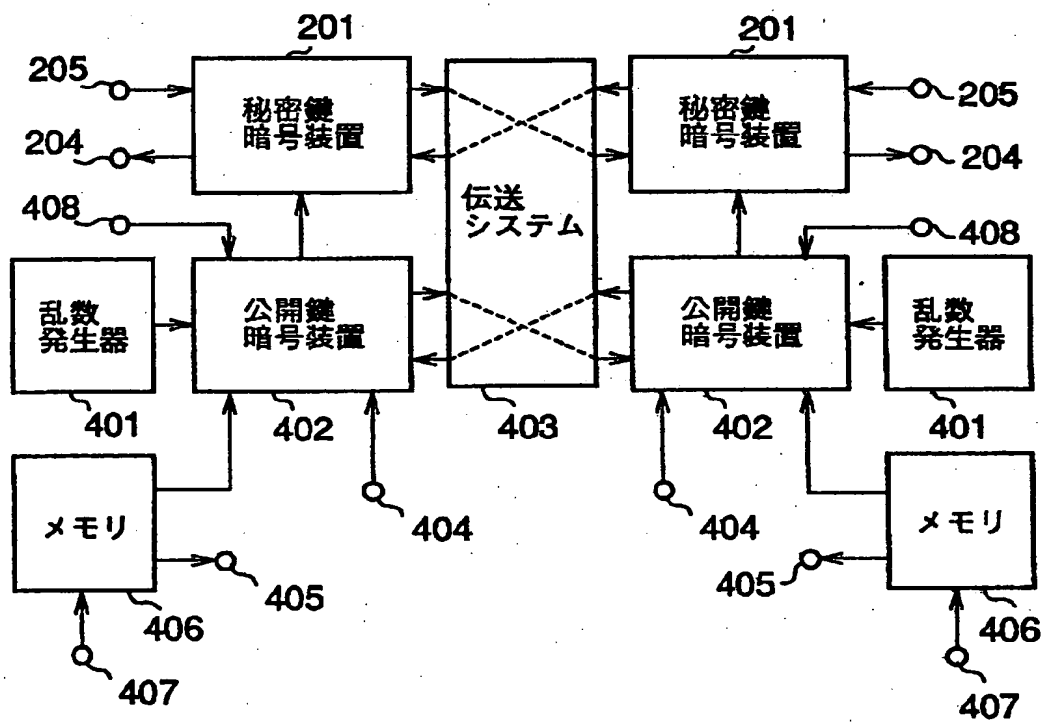
【図1】



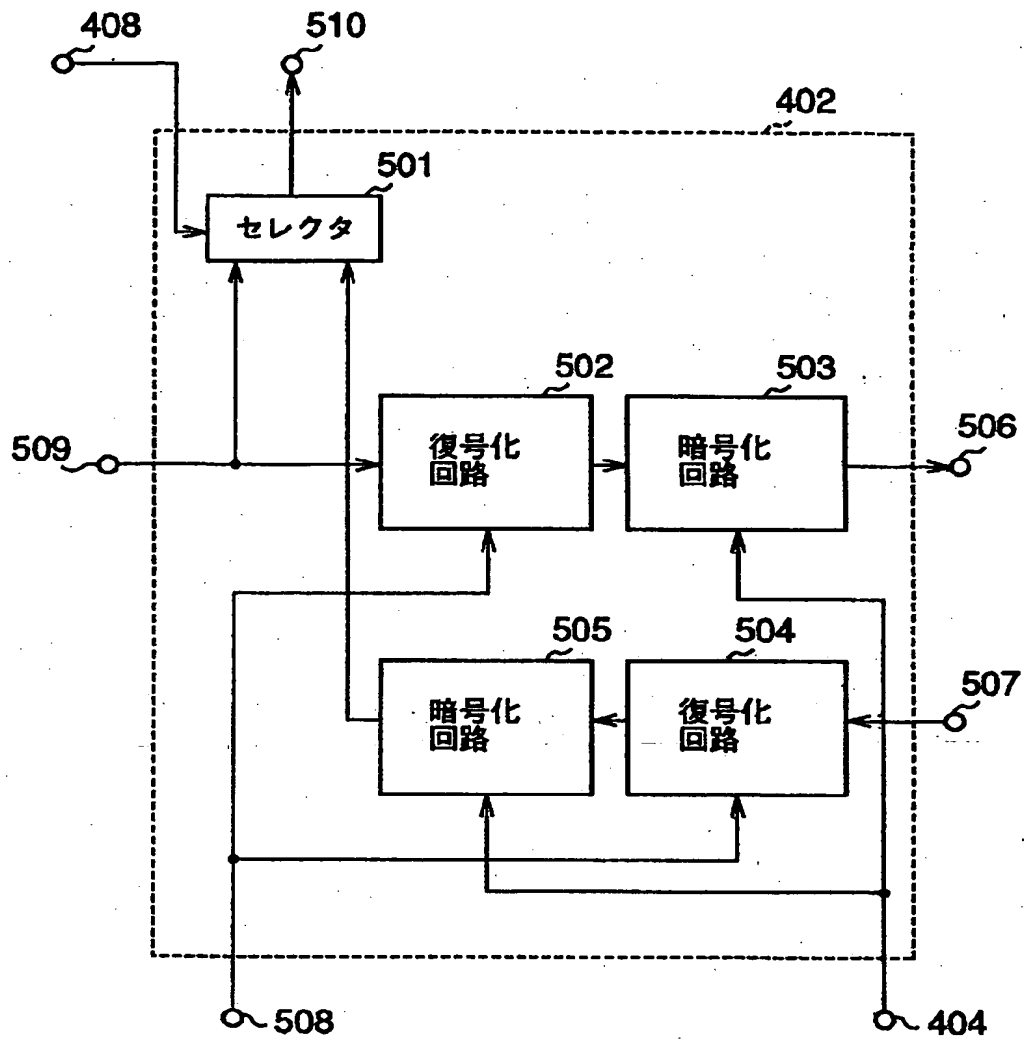
【図3】



【図4】



【図5】



フロントページの続き

(51) Int. Cl.⁵H04L 9/10
9/12

識別記号

庁内整理番号

F I

技術表示箇所